

On Quantum and Classical MDS-Convolutional BCH Codes

Giuliano G. La Guardia

Abstract—New families of classical and quantum convolutional Bose-Chaudhuri-Hocquenghem (BCH) codes are constructed algebraically in this paper. These classical (quantum) convolutional codes are optimal in the sense that they attain the classical (quantum) generalized Singleton bound. Additionally, such codes are non Reed-Solomon-type.

I. INTRODUCTION

Several works available in the literature deal with constructions of quantum error-correcting codes (QECC) [4–9, 13, 17, 21, 22, 24, 33, 41, 42]. In contrast with this subject of research one has the theory of quantum convolutional codes [1–3, 12, 14–16, 34, 35, 43–45]. Ollivier and Tillich [34, 35] were the first to develop the stabilizer structure for these codes. Almeida and Palazzo Jr. construct an $[[4, 1, 3]]$ (memory $m = 3$) quantum convolutional code [1]. Grassl and Rötteler [14–16] constructed quantum convolutional codes as well as they provide algorithms to obtain non-catastrophic encoders. Forney, in a joint work with Guha and Grassl, constructed rate $(n-2)/n$ quantum convolutional codes. Wilde and Brun [44, 45] constructed entanglement-assisted quantum convolutional coding and Tan and Li [43] constructed quantum convolutional codes derived from LDPC codes.

As can be seen, the latter class of codes has received less attention. Keeping this fact in mind, in this paper we propose constructions of new families of quantum and classical convolutional codes by applying the famous method proposed by Piret [36] and recently generalized by Aly *et al.* [2], which consists in the construction of (classical) convolutional codes derived from block codes. More precisely, we first construct new (classical) maximum-distance-separable (MDS) convolutional codes (in the sense that they attain the generalized Singleton bound [38, Theorem 2.2]). After this procedure we apply the well known technique by Aly *et al.* [2, Proposition 2] in order to construct new MDS convolutional stabilizer codes (in the sense that they attain the quantum generalized Singleton bound [3, Theorem 7]) derived from their classical counterparts.

An advantage of our procedure lies in the fact that all new (classical and quantum) convolutional codes are generated algebraically and not by computational search. Therefore, new families of classical and quantum convolutional codes are constructed, and not only specific codes. Additionally, our new (classical and quantum) convolutional MDS codes are non-Reed-Solomon type, in contrast with the most known (classical and quantum) convolutional codes available in the

literature. Moreover, as it is well known, in many works, only exhaustively computational search or even specific codes are constructed, that is, the codes are constructed case by case.

The constructions proposed here deal with suitable properties of cyclotomic cosets, that will be specified throughout this paper (see Sections V and VI). These nice properties of the cosets hold when considering classical convolutional codes of length $n = q + 1$ over the field F_q for all prime power q , or even quantum convolutional codes of length $n = q^2 + 1$ over F_{q^2} , where $q = 2^t$, $t \geq 3$ is an integer. In the quantum case, the corresponding classical codes are endowed with the Hermitian inner product.

The new families of classical convolutional codes have parameters

- $(n, n - 2i, 2; 1, 2i + 3)_q$, where $1 \leq i \leq \frac{q}{2} - 2$, $q = 2^t$, $t \geq 3$ is an integer, $n = q + 1$ is the code length, $k = n - 2i$ is the code dimension, $\gamma = 2$ is the degree of the code, $m = 1$ is the memory and $d_f = 2i + 3$ is the free distance of the code;
- $(n, n - 2i + 1, 2; 1, 2i + 2)_q$, where $q = p^t$, $t \geq 2$ is an integer, p is an odd prime number, $n = q + 1$ and $1 \leq i \leq \frac{n}{2} - 2$.

The quantum convolutional codes constructed in this paper have parameters

- $[[n, n - 4i, 1; 2, 2i + 3]]_q$, where $2 \leq i \leq \frac{q}{2} - 2$, $q = 2^t$, $t \geq 3$ is an integer and $n = q^2 + 1$. Here, n is the frame size, $k = n - 4i$ is the number of logical qudits per frame, $m = 1$ is the memory, $\gamma = 2$ is the degree and $d_f = 2i + 3$ is the free distance of the code.

Note that the parameters of classical convolutional codes differ from the parameters of the quantum convolutional codes. In particular, the order of the degree and the memory are changed.

Constructions of (classical) convolutional codes and their corresponding properties as well as constructions of optimal convolutional codes (in the sense that they attain the generalized Singleton bound [38]) have been also presented in the literature [11, 18, 28, 29, 36, 38–40]. In particular, in the paper by Rosenthal and York [39], the approach employed was to work with linear state-space descriptions in order to construct BCH convolutional codes, which is similar to the BCH (block) code construction.

As it is well known, the generalized (classical) Singleton bound [38] (see also [40]) appears recently in the literature. In the paper by Piret [37] and even in the handbook [36], the concept of MDS convolutional codes was addressed, but in a different context that the previously mentioned. In this paper we use the notion of MDS convolutional codes according to

Giuliano Gadioli La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil.

Smarandache and Rosenthal [40].

Let us now give the structure of the paper. In Section II, we review basic concepts on cyclic codes. In Section III, a review of concepts concerning classical and quantum convolutional codes is given. In Section IV, we propose constructions of new families of classical MDS convolutional codes and, in Section V, we construct new optimal (MDS) quantum convolutional codes. Finally, in Section VI, a brief summary is described.

II. REVIEW OF CYCLIC CODES

Notation. Throughout this paper, p denotes a prime number, q is a prime power and F_q is a finite field with q elements. The code length is denoted by n . As usual, the multiplicative order of q modulo n is given by $l = \text{ord}_n(q)$, α denotes a primitive n -th root of unity, and the minimal polynomial (over F_q) of an element $\alpha^j \in F_{q^m}$ is denoted by $M^{(j)}(x)$.

The notation C_s is utilized to denote a cyclotomic coset containing s , the code C^\perp denotes the Euclidean dual and the code C^{\perp_h} denotes the Hermitian dual of a given code C .

Let C be a cyclic code of length n over F_q . Then there exists only one monic polynomial $g(x)$ with minimal degree in C . Moreover, $C = \langle g(x) \rangle$, i. e., $g(x)$ is a generator polynomial of C and $g(x)$ is a factor of $x^n - 1$. The dimension of C equals $n - r$, where $r = \deg g(x)$.

Theorem 2.1: (The BCH bound)[32, pg. 201] Let α be a primitive n -th root of unity. Let C be a cyclic code with generator polynomial $g(x)$ such that, for some integers $b \geq 0$ and $\delta \geq 1$, and for $\alpha \in F_q$, we have $g(\alpha^b) = g(\alpha^{b+1}) = \dots = g(\alpha^{b+\delta-2}) = 0$, that is, the code has a sequence of $\delta - 1$ consecutive powers of α as zeros. Then the minimum distance of C is, at least, δ .

Definition 2.1: [32, pg. 202] Let α be a primitive n -th root of unity. A cyclic code C of length n over F_q is a BCH code with designed distance δ if, for some integer $b \geq 0$, we have

$$g(x) = \text{l.c.m.}\{M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+\delta-2)}(x)\},$$

that is, $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ as zeros. Therefore, $c \in C$ if and only if $c(\alpha^b) = c(\alpha^{b+1}) = \dots = c(\alpha^{b+\delta-2}) = 0$. Thus the code has a string of $\delta - 1$ consecutive powers of α as zeros. A parity check matrix for C is given by

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{(b+1)} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \dots & \dots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix},$$

where each entry is replaced by the corresponding column of l elements from F_q , where $l = \text{ord}_n(q)$, and then removing any linearly dependent rows. The rows of the resulting matrix over F_q are the parity checks satisfied by C .

Let $\mathcal{B} = \{b_1, \dots, b_l\}$ be a basis of F_{q^l} over F_q . If $u = (u_1, \dots, u_n) \in F_{q^l}^n$ then one can write the vectors u_i , $1 \leq i \leq n$, as linear combinations of the elements of \mathcal{B} , that is, $u_i = u_{i1}b_1 + \dots + u_{il}b_l$. Consider that $u^{(j)} = (u_{1j}, \dots, u_{nj})$

are vectors in F_q^n with $1 \leq j \leq l$. Then, if $v \in F_q^n$, one has $v \cdot u = 0$ if and only if $v \cdot u^{(j)} = 0$ for all $1 \leq j \leq l$.

From the BCH bound, the minimum distance of a BCH code is greater than or equal to its designed distance δ . If $n = q^l - 1$ then the BCH code is called primitive and if $b = 1$ it is called narrow-sense.

III. REVIEW OF CONVOLUTIONAL CODES

In this section we present a brief review of classical and quantum convolutional codes. For more details we refer the reader to [2, 3, 11, 19, 20, 36]. The following results can be found in [2, 3, 19, 20].

Recall that a polynomial encoder matrix $G(D) \in F_q[D]^{k \times n}$ is called *basic* if $G(D)$ has a polynomial right inverse.

A basic generator matrix of a convolutional code C is called *reduced* (or minimal [19, 29, 40]) if the overall constraint

length $\gamma = \sum_{i=1}^k \gamma_i$ has the smallest value among all basic generator matrices of C ; in this case the overall constraint length γ is called the *degree* of the code.

Definition 3.1: [3] A rate k/n convolutional code C with parameters $(n, k, \gamma; m, d_f)_q$ is a submodule of $F_q[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in F_q[D]^{k \times n}$, that is, $C = \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in F_q[D]^k\}$, where n is the length, k is the dimension, $\gamma = \sum_{i=1}^k \gamma_i$ is the *degree*, where $\gamma_i = \max_{1 \leq j \leq n} \{\deg g_{ij}\}$, $m = \max_{1 \leq i \leq k} \{\gamma_i\}$ is the *memory* and $d_f = \text{wt}(C) = \min\{\text{wt}(\mathbf{v}(D)) | \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ is the *free distance* of the code.

In the above definition, the *weight* of an element $\mathbf{v}(D) \in F_q[D]^n$ is defined as $\text{wt}(\mathbf{v}(D)) = \sum_{i=1}^n \text{wt}(v_i(D))$, where $\text{wt}(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$.

If one considers the field of Laurent series $F_q((D))$ whose elements are given by $\mathbf{u}(D) = \sum_i u_i D^i$, where $u_i \in F_q$ and $u_i = 0$ for $i \leq r$, for some $r \in \mathbb{Z}$, we define the weight of $\mathbf{u}(D)$ as $\text{wt}(\mathbf{u}(D)) = \sum_{\mathbb{Z}} \text{wt}(u_i)$. A generator matrix $G(D)$ is called *catastrophic* if there exists a $\mathbf{u}(D)^k \in F_q((D))^k$ of infinite Hamming weight such that $\mathbf{u}(D)^k G(D)$ has finite Hamming weight. Since a basic generator matrix is non-catastrophic, all the classical (quantum) convolutional codes constructed in this paper have non catastrophic generator matrices.

In this paper we construct unit memory (classical) MDS-convolutional codes, that is, MDS-convolutional codes generated by matrices G of the form $G = G_0 + G_1 D$. Such construction is performed algebraically. After this we construct new MDS quantum convolutional codes derived from their classical counterparts. Lee [25] was the first author to construct good unit memory convolutional codes; in fact he showed that such class of convolutional codes have large free distance when compared to multi-memory codes of same rate. This is the reason for which we restrict ourselves to the construction of unit memory convolutional codes.

Let us recall that the Euclidean inner product of two n -tuples $\mathbf{u}(D) = \sum_i u_i D^i$ and $\mathbf{v}(D) = \sum_j v_j D^j$ in $F_q[D]^n$ is

defined as $\langle \mathbf{u}(D) | \mathbf{v}(D) \rangle = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i$. If C is a convolutional code then the code $C^\perp = \{\mathbf{u}(D) \in F_q[D]^n \mid \langle \mathbf{u}(D) | \mathbf{v}(D) \rangle = 0 \text{ for all } \mathbf{v}(D) \in C\}$ denotes its Euclidean dual.

Similarly, the Hermitian inner product is defined as $\langle \mathbf{u}(D) | \mathbf{v}(D) \rangle_h = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i^q$, where $\mathbf{u}_i, \mathbf{v}_i \in F_{q^2}^n$ and $\mathbf{v}_i^q = (v_{1i}^q, \dots, v_{ni}^q)$. The Hermitian dual of the code C is defined by $C^{\perp_h} = \{\mathbf{u}(D) \in F_{q^2}[D]^n \mid \langle \mathbf{u}(D) | \mathbf{v}(D) \rangle_h = 0 \text{ for all } \mathbf{v}(D) \in C\}$.

A. Convolutional Codes Derived from Block Codes

In this subsection we recall some results shown in [2] that will be utilized in the proposed constructions.

We consider that $[n, k, d]_q$ is a block code with parity check matrix H and then we split H into $m+1$ disjoint submatrices H_i such that

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_m \end{bmatrix}, \quad (1)$$

where each H_i has n columns, obtaining the polynomial matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \dots + \tilde{H}_m D^m. \quad (2)$$

As it is well known, the matrix $G(D)$ generates a convolutional code with κ rows, where κ is the maximal number of rows among the matrices H_i ; the matrices \tilde{H}_i , where $1 \leq i \leq m$, are derived from the respective H_i ($1 \leq i \leq m$) by adding zero-rows at the bottom in such a way that the matrix \tilde{H}_i has κ rows in total. Note that the value m coincides with the notion of memory of a convolutional code (defined above) since the matrix \tilde{H}_m is the matrix with monomials of degree m .

Theorem 3.1: [2, Theorem 3] Suppose that $C \subseteq F_q^n$ is a linear code with parameters $[n, k, d]_q$ and assume also that $H \in F_q^{(n-k) \times n}$ is a parity check matrix for C partitioned into submatrices H_0, H_1, \dots, H_m as in eq. (1) such that $\kappa = \text{rk} H_0$ and $\text{rk} H_i \leq \kappa$ for $1 \leq i \leq m$ and consider the polynomial matrix $G(D)$ as in eq. (2). Then we have:

- (a) The matrix $G(D)$ is a reduced basic generator matrix;
- (b) If $C^\perp \subset C$ (resp. $C^{\perp_h} \subset C$), then the convolutional code $V = \{\mathbf{v}(D) = \mathbf{u}(D)G(D) \mid \mathbf{u}(D) \in F_q^{n-k}[D]\}$ satisfies $V \subset V^\perp$ (resp. $V \subset V^{\perp_h}$);
- (c) If d_f and d_f^\perp denote the free distances of V and V^\perp , respectively, d_i denote the minimum distance of the code $C_i = \{\mathbf{v} \in F_q^n \mid \mathbf{v} \tilde{H}_i^t = 0\}$ and d^\perp is the minimum distance of C^\perp , then one has $\min\{d_0 + d_m, d\} \leq d_f^\perp \leq d$ and $d_f \geq d^\perp$.

B. Review of Quantum Convolutional Codes

We begin this subsection by describing briefly the concept of quantum convolutional codes. For more details the reader can consult [2, 3, 12, 35].

Recall that an rate k/n quantum convolutional code C with parameters $[(n, k, m; \gamma, d_f)]_q$ is defined by a stabilizer matrix of the form

$$S(D) = (X(D) \mid Z(D)) \in F_q[D]^{(n-k) \times 2n}$$

satisfying $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$ (symplectic orthogonality), where n is the frame size, k is the number of logical qudits per frame, $m = \max_{1 \leq i \leq n-k, 1 \leq j \leq n} \{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$ is the memory, d_f is the free distance and γ is the degree of the code. Similarly as in the classical case, the constraint lengths are defined as $\gamma_i = \max_{1 \leq j \leq n} \{\max\{\deg X_{ij}(D), \deg Z_{ij}(D)\}\}$, and the overall constraint length is defined as $\gamma = \sum_{i=1}^{n-k} \gamma_i$.

Next, let $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \dots \otimes \mathbb{C}^q$ be the Hilbert space and $|x\rangle$ be the vectors of an orthonormal basis of \mathbb{C}^q , where the labels x are elements of F_q . Consider $a, b \in F_q$ and take the unitary operators $X(a)$ and $Z(b)$ in \mathbb{C}^q defined by $X(a)|x\rangle = |x+a\rangle$ and $Z(b)|x\rangle = w^{\text{tr}(bx)}|x\rangle$, respectively, where $w = \exp(2\pi i/p)$ is a primitive p -th root of unity, p is the characteristic of F_q and tr is the trace map from F_q to F_p . Considering the error basis $\mathbb{E} = \{X(a), Z(b) \mid a, b \in F_q\}$, one defines the set P_∞ (according to [3]) as the set of all infinite tensor products of matrices $N \in \langle M \mid M \in \mathbb{E} \rangle$, in which all but finitely many tensor components are equal to I , where I is the $q \times q$ identity matrix. Then one defines the weight wt of $A \in P_\infty$ as its (finite) number of nonidentity tensor components. In this context, one says that a quantum convolutional code has free distance d_f if and only if it can detect all errors of weight less than d_f , but cannot detect some error of weight d_f .

The following lemma deals with the existence of convolutional stabilizer codes derived from classical convolutional codes:

Lemma 3.2: [2, Proposition 2] Let C be an $(n, (n-k)/2, \gamma; m)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n, k, m; \gamma, d_f)]_q$ convolutional stabilizer code, where $d_f = \text{wt}(C^{\perp_h} \setminus C)$.

In [3], the authors derived the quantum Singleton bound for quantum convolutional codes as it is shown in the next theorem. Moreover, they constructed a family of optimal convolutional stabilizer codes (that is, codes attaining this bound) derived from (classical) generalized Reed-Solomon codes. Let C be an $[(n, k, m; \gamma, d_f)]_q$ quantum convolutional code. Recall that C is a pure code if does not exist errors of weight less than d_f in the stabilizer of C .

We will utilize the quantum Singleton bound in order to prove that our codes are MDS.

Theorem 3.3: (Quantum Singleton bound) The free distance of an $[(n, k, m; \gamma, d_f)]_q$ F_{q^2} -linear pure convolutional stabilizer code is bounded by

$$d_f \leq \frac{n-k}{2} \left(\left\lfloor \frac{2\gamma}{n+k} \right\rfloor + 1 \right) + \gamma + 1.$$

IV. NEW CLASSICAL MDS-CONVOLUTIONAL CODES

Constructions of MDS classical convolutional codes, that is, codes attaining the generalized Singleton bound (see [38]) is a difficult task [18, 28, 29, 36, 38, 40]. If one considers the optimality with respect to other existing bounds [27], some works in this direction has been done [10, 26, 30, 31]. We believe that the difficulty of constructing MDS convolutional

codes lies on the fact that the parameters of such codes are hard to be specified and also in the difficulty of constructing the corresponding MDS linear block codes. Due to the referred difficulty, most of methods available in the literature are based on computational search. Keeping in mind the discussion above, our purpose is to construct new families of classical and quantum MDS convolutional codes by applying algebraic methods.

The main results of this section are Theorems 4.2 and 4.7. They generate new families of optimal (in the sense that the codes attain the generalized Singleton bound [38]) convolutional codes of length $n = q + 1$, over F_q for all prime power q , of non Reed-Solomon-type. Before proceeding further, recall the well known result from [32]:

Lemma 4.1: [32, Theorem 9, Chapter 11] Suppose that $q = 2^t$, where $t \geq 2$ is an integer, $n = q + 1$ and consider that $a = \frac{q}{2}$. Then one has:

- i) With exception of coset $\mathcal{C}_0 = \{0\}$, each one of the other q -ary cyclotomic cosets is of the form $\mathcal{C}_{a-i} = \{a-i, a+i+1\}$, where $0 \leq i \leq a-1$;
- ii) The q -ary cosets $\mathcal{C}_{a-i} = \{a-i, a+i+1\}$, where $0 \leq i \leq a-1$, are mutually disjoint.

We are now able to show one of the main results of this section:

Theorem 4.2: Assume $q = 2^t$, where $t \geq 3$ is an integer, $n = q + 1$ and consider that $a = \frac{q}{2}$. Then there exist classical MDS convolutional codes with parameters $(n, n-2i, 2; 1, 2i+3)_q$, where $1 \leq i \leq \frac{q}{2} - 2$.

Proof: We first note that $\gcd(n, q) = 1$ and $\text{ord}_n(q) = 2$. The proof consists of two steps. The first one is the construction of suitable BCH (block) codes and the second step is the construction of convolutional BCH codes derived from the BCH (block) codes generated in the first step.

Let us begin the first step. Let C_2 be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_2 = \langle g_2(x) \rangle = \langle M^{(a-i)}(x)M^{(a-i+1)}(x) \cdot \dots \cdot M^{(a-1)}(x)M^{(a)}(x) \rangle.$$

A parity check matrix of C_2 is obtained from the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector (containing 2 rows) with respect to some F_q -basis β of F_{q^2} and then removing any linearly dependent rows. This new matrix H_{C_2} is a parity check matrix of C_2 and it has $2i+2$ rows. Since the dimension of C_2 is equal to $n-2(i+1)$ (as proved in the paragraph below), then H_{C_2} has rank $2i+2$, so there is no linearly dependent rows in H_{C_2} .

From Lemma 4.1, each one of the q -ary cyclotomic cosets \mathcal{C}_{a-i} , where $0 \leq i \leq a-1$ (corresponding to the minimal

polynomials $M^{(a-i)}(x)$), has two elements and they are mutually disjoint. Since the degree of the generator polynomial $g_2(x)$ of the code C_2 equals the cardinality of its defining set, then one has $\deg(g_2(x)) = 2(i+1)$, so the dimension k_{C_2} of C_2 equals $k_{C_2} = n - \deg(g_2(x)) = n - 2(i+1)$. Moreover, the defining set of the code C_2 consists of the sequence $\{a-i, a-i+1, \dots, a, a+1, \dots, a+i+1\}$ of $2i+2$ consecutive integers, so, from the BCH bound, the minimum distance d_{C_2} of C_2 satisfies $d_{C_2} \geq 2i+3$. Thus, C_2 is a MDS code with parameters $[n, n-2i-2, 2i+3]_q$. Since C_2 has dimension $n-2i-2$, then its (Euclidean) dual code has dimension $2i+2$.

We next consider that C_1 is the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_1 = \langle g_1(x) \rangle = \langle M^{(a-i+1)}(x)M^{(a-i+2)}(x) \cdot \dots \cdot M^{(a-1)}(x)M^{(a)}(x) \rangle.$$

Similarly, C_1 has a parity check matrix derived from the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \dots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \end{bmatrix}$$

by expanding each entry as a column vector (containing 2 rows) with respect to β (already done, since $H_{2i+1, a-i+1}$ is a submatrix of $H_{2i+3, a-i}$). After performing the expansion to all entries, such new matrix is denoted by H_{C_1} (H_{C_1} is a submatrix of H_{C_2}). Applying again Lemma 4.1 and proceeding similarly as above, it follows that C_1 is a MDS code with parameters $[n, n-2i, 2i+1]_q$. Since C_1 has dimension $n-2i$, then its (Euclidean) dual code has dimension $2i$, so H_{C_1} has rank $2i$.

To finish the first step, consider C be the BCH code of length n over F_q generated by the minimal polynomial $M^{(a-i)}(x)$, that is,

$$C = \langle M^{(a-i)}(x) \rangle.$$

C has parameters $[n, n-2, d \geq 2]_q$. A parity check matrix H_C of C is given by expanding each entry of the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \end{bmatrix}$$

with respect to β (already done, since $H_{2, a-i}$ is a submatrix of $H_{2i+3, a-i}$). Since C has dimension $n-2$, H_C has rank 2 (H_C is also a submatrix of H_{C_2}).

Next we describe the second step. We begin by rearranging

the rows of H_{C_2} in the form

$$H = \begin{bmatrix} 1 & \alpha^a & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

where $a = \frac{q}{2}$ (to simplify the notation we write H in terms of powers of α , although it is clear from the context that this matrix has entries in F_q , which are derived from expanding each entry with respect to the basis β already performed)

Then we split H into two disjoint submatrices H_0 and H_1 of the forms

$$H_0 = \begin{bmatrix} 1 & \alpha^a & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \end{bmatrix}$$

and

$$H_1 = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

respectively, where H_0 is obtained from the matrix H_{C_1} by rearranging rows and H_1 is derived from H_C also by rearranging rows. Hence it follows that $\text{rk} H_0 \geq \text{rk} H_1$.

Then we form the convolutional code V generated by the reduced basic (according to Theorem 3.1 Item (a)) generator matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D,$$

where $\tilde{H}_0 = H_0$ and \tilde{H}_1 is obtained from H_1 by adding zero-rows at the bottom such that \tilde{H}_1 has the number of rows of H_0 in total. By construction, V is a unit memory convolutional code of dimension $2i$ and degree $\delta_V = 2$.

Consider next the Euclidean dual V^\perp of the convolutional code V . We know that V^\perp has dimension $n - 2i$ and degree 2. Let us now compute the free distance d_f^\perp of V^\perp . By Theorem 3.1 Item (c), the free distance of V^\perp is bounded by $\min\{d_0 + d_1, d\} \leq d_f^\perp \leq d$, where d_i is the minimum distance of the code $C_i = \{\mathbf{v} \in F_q^n \mid \mathbf{v} \tilde{H}_i^t = 0\}$. From construction one has $d = 2i + 3$, $d_0 = 2i + 1$ and $d_1 \geq 2$, so V^\perp has parameters $(n, n - 2i, 2; 1, 2i + 3)_q$.

Recall that the generalized (classical) Singleton bound [40] of an $(n, k, \gamma; m, d_f)_q$ convolutional code is given by

$$d_f \leq (n - k)[\lceil \gamma/k \rceil + 1] + \gamma + 1.$$

Replacing the values of the parameters of V^\perp in the above inequality one concludes that V^\perp is a MDS convolutional code. We finish by observing that such codes are non Reed-Solomon-type. ■

Remark 4.3: It is interesting to observe that the convolutional codes constructed in Theorem 4.2 have unit memory. This is due to the fact that such class of codes have large free

distance when compared to multi-memory codes of same rate (see [25]).

Remark 4.4: Note that the new codes have degree $\gamma = 2$. The reason for this is as follows: in order to obtain codes with maximum minimum distances we have to construct codes (the notation is the same utilized in Theorem 4.2) satisfying the inequalities $\min\{d_0 + d_1, d\} \leq d_f^\perp \leq d$. Therefore one designs the code C with parameters $[n, n - 2, d_1 \geq 2]_q$. Now, it is easy to see that the corresponding convolutional code V^\perp has degree 2, because V has degree 2 and the matrix H_1 has 2 linearly independent rows.

Let us now give an illustrative example.

Example 4.1: According to Theorem 4.2, let $q = 16$, $n = q + 1 = 17$ and $a = 8$. Assume C_2 is an $[17, 11, 7]_{16}$ (cyclic) MDS code generated by the product of the minimal polynomials $M^{(8)}(x)M^{(7)}(x)M^{(6)}(x)$. The corresponding cyclotomic cosets of C_2 are $\{8, 9\}$, $\{7, 10\}$ and $\{6, 11\}$. Consider C_1 be the (cyclic) MDS code generated by the product of the minimal polynomials $M^{(8)}(x)M^{(7)}(x)$; C_1 has parameters $[17, 13, 5]_{16}$. Finally, suppose C is the cyclic code generated by $M^{(6)}(x)$, where C has parameters $[17, 15, d \geq 2]_{16}$. In this case we have $i = 2$. Then we can form the convolutional code V with reduced basic generator matrix $G(D) = \tilde{H}_0 + \tilde{H}_1 D$, where $\tilde{H}_0 = H_0$ and \tilde{H}_1 is obtained from H_1 by adding zero-rows at the bottom such that \tilde{H}_1 has the number of rows of H_0 in total. The matrix H_0 is the parity check matrix of C_1 (up to permutation of rows) and H_1 is the parity check matrix of C . V has parameters $(17, 4, 2; 1, d_f)_{16}$. The Euclidean dual V^\perp has parameters $(17, 13, 2; 1, d_f^\perp)_{16}$, where $\min\{d_0 + d_1, d\} \leq d_f^\perp \leq d$, where $d_0 = 5$, $d_1 \geq 2$ and $d = 7$. Therefore V^\perp has parameters $(17, 13, 2; 1, 7)_{16}$. Applying the generalized Singleton bound one has $7 = 4(\lfloor 2/13 \rfloor + 1) + 2 + 1$, so V^\perp is MDS.

It is well known (see for example [38]) that if a convolutional code C is MDS then one can not guarantee that its dual also is MDS. Unfortunately in the above construction, although the codes V^\perp are MDS, there is no guarantee that their duals V are MDS:

Corollary 4.5: Assume $q = 2^t$, where $t \geq 3$ is an integer, $n = q + 1$ and consider that $a = \frac{q}{2}$. Then there exist classical convolutional codes with parameters $(n, 2i, 2; 1, d_f)_q$, where $1 \leq i \leq \frac{q}{2} - 2$ and $d_f \geq n - 2i - 1$.

Proof: Consider the same construction and notation used in Theorem 4.2. We know that V has parameters $(n, 2i, 2; 1, d_f)_q$. Let us compute d_f . From Theorem 3.1 Item (b), $d_f \geq d^\perp$. We know that the matrix H is obtained by rearranging the rows of H_{C_2} and the code C_2^\perp is a MDS code with parameters $[n, 2i + 2, n - 2i - 1]_q$. Thus $d_f \geq n - 2i - 1$ and V has parameters $(n, 2i, 2; 1, d_f)_q$, where $d_f \geq n - 2i - 1$. ■

Theorem 4.7, given in the sequence, is the second main result of this section. More precisely, in such theorem, we construct new families of (classical) convolutional codes over F_q for all $q = p^t$, where $t \geq 2$ and p is an odd prime number. In order to prove it, we need the following well known result:

Lemma 4.6: [32, Theorem 9, Chapter 11] Suppose that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Let $n = q + 1$ and consider that $a = \frac{n}{2}$. Then one has:

- i) The q -ary coset C_a has only one element, that is, $C_a = \{a\}$;
- ii) With exception of cosets $C_0 = \{0\}$ and C_a , each one of the other q -ary cyclotomic cosets is of the form $C_{a-i} = \{a-i, a+i\}$, where $1 \leq i \leq a-1$;
- iii) The q -ary cosets $C_{a-i} = \{a-i, a+i\}$, where $1 \leq i \leq a-1$, are mutually disjoint and have two elements.

Let us now prove Theorem 4.7. Since its proof is analogous to that of Theorem 4.2, we only give a sketch of it.

Theorem 4.7: Assume that $q = p^t$, where $t \geq 2$ is an integer and p is an odd prime number. Consider that $n = q+1$ and that suppose that $a = \frac{n}{2}$. Then there exist classical MDS convolutional codes with parameters $(n, n-2i+1, 2; 1, 2i+2)_q$, where $1 \leq i \leq \frac{n}{2}-2$.

Proof: Let C_2 be the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_2 = \langle g_2(x) \rangle = \langle M^{(a-i)}(x)M^{(a-i+1)}(x) \dots M^{(a-1)}(x)M^{(a)}(x) \rangle.$$

whose parity check matrix H_{C_2} is obtained from the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \end{bmatrix}^{H_{2i+2,a-i} =}$$

by expanding each entry as a column vector over some F_q -basis β of F_{q^2} .

From Lemma 4.6, each one of the q -ary cyclotomic cosets C_{a-i} , where $1 \leq i \leq a-1$, has two elements, they are mutually disjoint and the coset C_a has only one element. Thus the dimension k_{C_2} of C_2 equals $k_{C_2} = n - \deg(g_2(x)) = n - 2i - 1$. Moreover, since the defining set of the code C_2 consists of the sequence $\{a-i, a-i+1, \dots, a, a+1, \dots, a+i\}$ of $2i+1$ consecutive integers then the minimum distance d_{C_2} of C_2 satisfies $d_{C_2} \geq 2i+2$. Hence, C_2 is a MDS code with parameters $[n, n-2i-1, 2i+2]_q$ and H_{C_2} has rank $2i+1$.

We next consider C_1 as the BCH code of length n over F_q generated by the product of the minimal polynomials

$$C_1 = \langle g_1(x) \rangle = \langle M^{(a-i+1)}(x)M^{(a-i+2)}(x) \dots M^{(a-1)}(x)M^{(a)}(x) \rangle.$$

whose parity check matrix H_{C_1} is derived from the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \dots & \alpha^{(n-1)(a-i+2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \end{bmatrix}^{H_{2i,a-i+1} =}$$

by expanding each entry as a column vector with respect to β of F_{q^2} . Then it follows that C_1 is a MDS code with parameters $[n, n-2i+1, 2i]_q$ and H_{C_1} has rank $2i-1$.

Assume that C is the BCH code generated by the minimal polynomial $M^{(a-i)}(x)$. Then C has parameters $[n, n-2, d \geq 2]_q$. A parity check matrix H_C of C is given by expanding each entry of the matrix

$$= \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \end{bmatrix}^{H_{2,a-i} =}$$

with respect to β . H_C has rank 2.

Rearranging the rows of H_{C_2} we obtain the matrix

$$H = \begin{bmatrix} 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

where $a = \frac{n}{2}$. Next we split H into two disjoint submatrices H_0 and H_1 (as in Theorem 4.2) of the form

$$H_0 = \begin{bmatrix} 1 & \alpha^a & \dots & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \end{bmatrix}$$

and

$$H_1 = \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

obtaining, in this way, the convolutional code V generated by the matrix

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D$$

with parameters $(n, 2i-1, 2; 1, d_f)_q$. Proceeding similarly as in Theorem 4.2, one has a MDS convolutional code V^\perp with parameters $(n, n-2i+1, 2; 1, 2i+2)_q$, for all $1 \leq i \leq \frac{n}{2}-2$. These codes are non Reed-Solomon-type ■

V. NEW QUANTUM MDS-CONVOLUTIONAL CODES

As in the classical case, the construction of MDS quantum convolutional codes is a difficult task. This task is performed in [3, 12, 14, 16] but only in [3, 14] the constructions are made algebraically. Based on this view point, we propose the construction of more MDS convolutional stabilizer codes.

It is well known that convolutional stabilizer codes can be constructed from classical convolutional codes (see for example [2, Proposition 1 and 2]). In the first construction, one utilizes convolutional codes endowed with the Euclidean inner product and in the second one, the codes are endowed with the Hermitian inner product. Considering the q -ary cosets modulo $n = q+1$ as given in the previous section, it is easy to see that the self-orthogonality with respect to the Euclidean inner product does not hold for (classical) convolutional codes derived from block codes with defining set of this type. However, when considering cyclic codes endowed with the Hermitian inner

product one can show the existence of convolutional codes, derived from them, which are (Hermitian) self-orthogonal (see Lemma 5.1). This fact permits the construction of MDS quantum convolutional codes (in the sense that they attain the generalized quantum Singleton bound (Theorem 3.3) as it is shown in Theorem 5.2, given in the following. More precisely, we utilize the MDS-convolutional codes constructed in the previous section for constructing quantum MDS convolutional codes. Before proceeding further, we need the following result:

Lemma 5.1: Assume $q = 2^t$, where t is an integer such that $t \geq 1$, $n = q^2 + 1$ and let $a = \frac{q^2}{2}$. If C is the cyclic code whose defining set Z is given by $Z = \mathcal{C}_{a-i} \cup \dots \cup \mathcal{C}_a$, where $0 \leq i \leq \frac{q}{2} - 1$, then C is Hermitian self-orthogonal.

Proof: See [23, Lemma 4.2]. ■

Although Theorem 5.2 is a Corollary of Theorem 4.2, we consider it as a theorem because the resulting quantum convolutional codes are MDS.

Theorem 5.2: Assume $q = 2^t$, where $t \geq 3$ is an integer, $n = q^2 + 1$ and consider that $a = \frac{q^2}{2}$. Then there exist quantum MDS convolutional codes with parameters $[(n, n - 4i, 1; 2, 2i + 3)]_q$, where $2 \leq i \leq \frac{q}{2} - 2$.

Proof: We consider the same notation utilized in Theorem 4.2. We know that $\gcd(n, q^2) = 1$. From Theorem 4.2, there exists a classical convolutional MDS code with parameters $(n, n - 2i, 2; 1, 2i + 3)_{q^2}$, for each $2 \leq i \leq \frac{q}{2} - 2$. This code is the Euclidean dual V^\perp of the convolutional code V whose parameters are given by $(n, 2i, 2; 1, d_f)_{q^2}$. The codes V^\perp and V^{\perp_h} have the same degree as code (see the proof of Theorem 7 in [3]). Additionally, it is straightforward to check that $\text{wt}(V^\perp) = \text{wt}(V^{\perp_h})$, so V^{\perp_h} has parameters $(n, n - 2i, 2; m^*, 2i + 3)_{q^2}$. From Lemma 5.1 and from Theorem 3.1 Item (b), one has $V \subset V^{\perp_h}$. Applying Lemma 3.2, there exists an $[(n, n - 4i, 1; 2, d_f \geq 2i + 3)]_q$ convolutional stabilizer code, for each $2 \leq i \leq \frac{q}{2} - 2$. Replacing the parameters of the previously constructed codes in the quantum generalized Singleton bound (Theorem 3.3) one has the equality $2i + 3 = 2i \left(\left\lfloor \frac{4}{2n - 4i} \right\rfloor + 1 \right) + 2 + 1$. Therefore, there exist MDS-convolutional stabilizer codes with parameters $[(n, n - 4i, 1; 2, 2i + 3)]_q$, for each $2 \leq i \leq \frac{q}{2} - 2$. Note that these quantum MDS codes are non Reed-Solomon-type. ■

Example 5.1: To illustrate the previous construction, assume that $q = 8$, $n = 65$ and $i = 2$. Applying Theorem 5.2 there exists an $[(65, 57, 1; 2, 7)]_8$ convolutional stabilizer code that attains the generalized quantum Singleton bound.

Considering $q = 16$, $n = 257$ and $i = 2, 3, 4, 5$ then one has quantum MDS codes with parameters $[(257, 249, 1; 2, 7)]_{16}$, $[(257, 245, 1; 2, 9)]_{16}$, $[(257, 241, 1; 2, 11)]_{16}$, $[(257, 237, 1; 2, 13)]_{16}$, respectively, and so on.

VI. SUMMARY

In this paper we have constructed, by means of an algebraic method, new families of classical and quantum convolutional BCH codes. These codes are optimal in the sense that they attain the quantum and classical generalized Singleton bound, respectively. In contrast with most codes available in the

literature, the new codes constructed here are non Reed-Solomon-type.

ACKNOWLEDGMENT

I would like to thank the anonymous referees for their valuable comments and suggestions that improve significantly the quality and the presentation of this paper. This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

REFERENCES

- [1] A. C. A. de Almeida and R. Palazzo Jr.. A concatenated $[(4, 1, 3)]$ quantum convolutional code. In *Proc. IEEE Inform. Theory Workshop (ITW)*, pp. 28–33, 2004.
- [2] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli. Quantum convolutional BCH codes. e-print arXiv:quant-ph/0703113.
- [3] S. A. Aly, A. Klappenecker, P. K. Sarvepalli. Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes. e-print arXiv:quant-ph/0701037.
- [4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(3):1183–1188, March 2007.
- [5] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, November 2001.
- [6] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000.
- [7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, July 1998.
- [8] H. Chen, S. Ling, and C. P. Xing. Quantum codes from concatenated algebraic geometric codes. *IEEE Trans. Inform. Theory*, 51(8):2915–2920, august 2005.
- [9] G. D. Cohen, S. B. Encheva, and S. Litsyn. On binary constructions of quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2495–2498, July 1999.
- [10] J. J. Climent, V. Herranz, C. Perea. Linear system modelization of concatenated block and convolutional codes. *Linear Algebra and its Applications*, 429(5-6):1191–1212, 2008.
- [11] G. D. Forney Jr. Convolutional codes I: algebraic structure. *IEEE Trans. Inform. Theory*, 16(6):720–738, November 1970.
- [12] G. D. Forney Jr., M. Grassl, S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inform. Theory*, 53(3):865–880, March 2007.
- [13] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Int. J. Quantum Inform.*, 2(1):757–766, 2004.
- [14] M. Grassl and M. Rötteler. Quantum block and convolutional codes from self-orthogonal product codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1018–1022, 2005.
- [15] M. Grassl and M. Rötteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1109–1113, 2006.
- [16] M. Grassl and M. Rötteler. Constructions of quantum convolutional codes. e-print arXiv:quant-ph/0703182.
- [17] M. Hamada. Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction. *IEEE Trans. Inform. Theory*, 54(12):5689–5704, December 2008.
- [18] K. J. Hole. On classes of convolutional codes that are not asymptotically catastrophic. *IEEE Trans. Inform. Theory*, 46(2):663–669, March 2000.
- [19] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.
- [20] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding*. Digital and Mobile Communication, Wiley-IEEE Press, 1999.
- [21] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, November 2006.
- [22] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A*, 80(4):042331(1–11), October 2009.
- [23] G. G. La Guardia. New quantum MDS codes. *IEEE Trans. Inform. Theory*, 57(8):5551–5554, August 2011.
- [24] G. G. La Guardia and R. Palazzo Jr.. Constructions of new families of nonbinary CSS codes. *Discrete Math.*, 310(21):2935–2945, November 2010.

- [25] L. N. Lee. Short unit-memory byte-oriented binary convolutional codes having maximum free distance. *IEEE Trans. Inform. Theory*, 22:349–352, May 1976.
- [26] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.
- [27] H. Gluesing-Luerssen, W. Schmale. Distance bounds for convolutional codes and some optimal codes. e-print arXiv:math/0305135.
- [28] H. Gluesing-Luerssen and W. Schmale. On doubly-cyclic convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 17(2):151–170, 2006.
- [29] H. Gluesing-Luerssen and F-L Tsang. A matrix ring description for cyclic convolutional codes. *Advances in Math. Communications*, 2(1):55–81, 2008.
- [30] R. Hutchinson, J. Rosenthal and R. Smarandache. Convolutional codes with maximum distance profile. *Systems and Control Letters*, 54(1):53–63, 2005.
- [31] J. I. Iglesias-Curto. Generalized AG Convolutional Codes. *Advances in Mathematics of Communications*, 3(4):317–328, 2009.
- [32] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [33] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [34] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):17790214, 2003.
- [35] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: fundamentals. e-print arXiv:quant-ph/0401134.
- [36] Ph. Piret. *Convolutional Codes: An Algebraic Approach*. Cambridge, Massachusetts: The MIT Press, 1988.
- [37] Ph. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.
- [38] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 10:15–32, 1998.
- [39] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833–1844, 1999.
- [40] R. Smarandache, H. G.-Luerssen, J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, July 2001.
- [41] P. K. Sarvepalli and A. Klappenecker. Nonbinary quantum Reed-Muller codes. In *Proc. Int. Symp. Inf. Theory (ISIT)*, pp. 1023–1027, 2005.
- [42] A. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, November 1999.
- [43] P. Tan and J. Li. Efficient Quantum Stabilizer Codes: LDPC and LDPC-Convolutional Constructions. *IEEE Trans. Inform. Theory*, 56(1):476–491, January 2010.
- [44] M. M. Wilde and T. A. Brun. Unified quantum convolutional coding. In *Proc. Int. Symp. Inf. Theory (ISIT)*, pp. 359–363, 2008.
- [45] M. M. Wilde and T. A. Brun. Entanglement-assisted quantum convolutional coding. *Phys. Rev. A*, 81(4):042333, April 2010.